UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Docket No. 21-cr-30028-MGM
	)	
BENJAMIN SHACAR	)	

MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (REDACTED)

The defendant, Benjamin Shacar, pursuant to Fed. R. Crim. P. 12 and the Fourth Amendment, has filed a motion that this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because the warrant was not supported by probable cause. Mr. Shacar has also moved for a *Franks* hearing, as the affiant made material misstatements that were necessary to a finding of probable cause and omissions that, if included in the affidavit, would have vitiated probable cause.

Pursuant to Local Rule 7(b)(1), Mr. Shacar files this memorandum in support of the motion to suppress evidence.

STATEMENT OF FACTS[1]

I. The Search Warrant

On March 22, 2021, Homeland Security Investigations ("HSI") Special Agent Daniel Yon applied for a search warrant to the U.S. District Court of Massachusetts. *See* Search Warrant Affidavit (attached as Ex. 1). Agent Yon sought authorization to search Mr. Shacar's home located in Pittsfield, Massachusetts for evidence, fruits, and instrumentalities of violations of 1) 18 U.S.C. §§ 2252(a)(1) and (b)(1) (Transportation of a Visual Depiction of a Minor Engaged in Sexually

[1] The facts in this section are drawn from the discovery and disclosures provided by the government. By repeating the facts here, Mr. Shacar does not adopt them as true.

Explicit Conduct); 2) 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Receipt or Distribution of a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct); 3) 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View a Visual Depiction of a Minor Engaged in Sexually Explicit Conduct); 4) 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (Transportation of Child Pornography); 5) 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Receipt or Distribution of Child Pornography); and 5) 18 U.S.C. §§2252A(a)(5)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography). Ex. 1 at ¶ 4.

The affidavit submitted in support of the search warrant alleged that there was probable cause to believe that a user of the internet account at Mr. Shacar's home had accessed on a single date in August, 2019, a Tor hidden-services website geared towards the sexual exploitation of minors. Agent Yon identified the target website in his affidavit. Specifically, Agent Yon stated:

> In August 2019, a foreign law enforcement agency (hereinafter, "FLA") known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that the FLA had determined that on May 2, 2019, IP address 24.194.90.108 was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as the TARGET WEBSITE.

Id. at ¶ 32. Agent Yon stated that the "FLA described the website facilitating 'the sharing of child sexual abuse and exploitation material stipulating only girls aged 5-13. Users were required to enter a username and password, but these were only valid for that single login session' and provided further documentation naming the website as the TARGET WEBSITE, which the FLA referred to by its actual name."[2]. *Id* at ¶ 33.

Agent Yon also included a description of how the Tor network operates and how information is anonymized on the network, noting that "the Tor network attempts to [facilitate anonymous

[2] Agent Yon noted in the affidavit that the FLA "referred to the site by its actual name." Ex. 1 at ¶ 33. The government has since disclosed that the website was called [GirLand]

communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit.'" *Id*. at ¶ 9. Agent Yon acknowledged that because of this process, "traditional IP address-based identification techniques are not effective," but he neither expounded on the methodology used to identify the suspect user IP address in this case, nor provided any explanation for the reliability of the identification of the suspect user IP address. *Id*.

In the section of the affidavit discussing the FLA tips, Agent Yon claimed that the FLA (later identified by the government in response to defense discovery requests as [redacted]) was a "national law enforcement agency of a country with an established rule of law." *Id*. at ¶ 34. Agent Yon averred that there was a "long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." *Id*. Agent Yon also stated that the FLA "had obtained that [tip] information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." *Id*. He further noted that the FLA had "advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information." *Id*. He stated that "U.S. law enforcement did not participate in the investigative work through which FLA identified the IP address." *Id*.

Finally, Agent Yon alleged that prior tips provided by the FLA had:

> (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

Id. at ¶ 35.

According to the affidavit, in March 2020, U.S. law enforcement sent a subpoena to Charter Communications for subscriber information related to the suspect user IP address. *Id*. at ¶ 41. Charter Communications provided law enforcement with a physical address – [redacted] associated with the IP address as well as the customer name – Benjamin Shacar. *Id*. Agent Yon stated that a search of a public records database and RMV records indicated that Benjamin Shacar lived at that address. Additional RMV records indicated that a car registered to Mr. Shacar and another car registered to both Mr. Shacar and his wife, [redacted], were registered to both subjects at the address listed above. *Id*. at ¶¶ 42-43. Agent Yon also noted that on December 10, 2020 and January 14, 2021, surveillance disclosed the vehicles at the premises referenced above. *Id*. at ¶¶ 44-45. Agent Yon also stated that representatives of Eversource Energy indicated that service was being provided to Benjamin Shacar at the same address and that a check with the United States Postal Service showed that Benjamin Shacar was receiving mail at that address. *Id*. at ¶¶ 46-47. Agent Yon included the fact that a check of open-source information from the internet showed a Facebook page for Benjamin Shacar which displays a profile picture of a man and woman together. The male depicted in the picture matches Mr. Shacar's RMV photograph, and the female matches Mrs. Shacar's RMV photograph. In addition a Facebook page for Desiree Shacar depicts a photograph of a female matching [redacted]'s RMV photograph. Another photo on the Facebook page shows a photograph of a woman holding a young child outdoors, near a house matching the description of [redacted], as well as the subject premises. *Id*. at ¶¶ 48-49.

A warrant to search Mr. Shacar's home was issued on March 22, 2021. *See* Search Warrant (attached as Ex. 2). The warrant was executed on March 24, 2021. Based on the evidence discovered at Mr. Shacar's home, Mr. Shacar was arrested and a complaint was filed alleging a

violation of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography). Mr. Shacar was later indicted on ten counts of receipt of child pornography and one count of possession of child pornography.

II. Information Omitted from the Affidavit

In response to specific defense discovery requests, the government disclosed that the FLA that provided the tip to U.S. law enforcement was the [redacted]. The defendant has requested information from the government as to whether the FLA providing the tip was the same FLA who seized the server hosting the website in question and the country where the server was located. The government has declined to identify whether a second FLA was involved with the seizure of the server or the server host country.

The defense has uncovered additional information not included in Agent Yon's affidavit that is material to the probable cause analysis. First, undersigned counsel has identified multiple cases from across the country that rely on similar August 2019 tips from an undisclosed FLA that an IP address was used to visit a Tor hidden services website sometime in April or May 2019. See Ex. 3 - 9. The number of similar cases using similar, if not identical, language to the search warrant affidavit in Mr. Shacar's case indicates a large-scale, coordinated investigation into websites hosted on the Tor network akin to the Playpen investigation.[3]

None of this information was included in Agent Yon's affidavit.

ARGUMENT

I. The Warrant Was Not Supported by Probable Cause.

The Fourth Amendment of the United States Constitution guarantees the right to be secure against "unreasonable searches and seizures" and requires that no warrants issue "but

[3]See "The Playpen Cases: Mass Hacking by U.S. Law Enforcement," Electronic Frontier Foundation, available at https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement.

upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched." U.S. Const. Am. IV. "With limited exceptions, it requires police officers to secure a search warrant supported by probable cause prior to effecting a search or seizure." *United States v. Gifford*, 727 F.3d 92, 98 (1st Cir. 2013).

Probable cause to issue a search warrant exists when "given all the circumstances set forth in the affidavit … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." Id. at 239. This Court is tasked with "ensur[ing] that the magistrate had a substantial basis for ... concluding that probable cause existed." Id. at 238-39.

When an affidavit relies on information provided by a confidential informant, "the affidavit must provide some information from which a magistrate can credit the informant's credibility." *Gifford*, 727 F.3d at 99. The First Circuit applies the following non-exhaustive factors in assessing probable cause in cases involving confidential tips:

> (1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant's statements reflect first-hand knowledge; (3) whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant's provided information.

United States v. Tiem Trinh, 665 F.3d 1, 10 (1st Cir. 2011).

Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Shacar's home. *Gates*, 462 U.S. at 238-39. The affidavit relied entirely on two unsubstantiated and stale allegations of criminal

activity by an unidentified foreign law enforcement agency (now known as [redacted]). The affidavit failed to include any information as to how the FLA came across that information, how reliable the method the FLA used to obtain the information was (if indeed it was that FLA that de-anonymized the suspect user IP address here), and whether the IP address and/or other tip information was obtained through the FLA's first-hand knowledge or through other sources. Without more information about the source of the FLA's tip and without additional corroboration, the twenty-two-month-old tip was not sufficient to establish probable cause.

a. The FLA Tip Was Insufficient to Establish Probable Cause.

The factors outlined by the First Circuit in *Tiem Trinh*, 665 F.3d at 10, are instructive in this case because the tip that forms the entire basis of probable cause in the affidavit came from a confidential source akin to an informant. Those factors, although non-exhaustive, weigh in Mr. Shacar's favor. Agent Yon's affidavit is deficient because 1) it fails to allege a crime; 2) it fails establish the basis of knowledge for the tip and whether it was obtained through first-hand knowledge or through hearsay (factors 1 and 2 in the Tiem Trinh analysis), and 3) it reflects no attempts from any U.S. law enforcement agency to corroborate the tip from the unidentified FLA (factor 3 of Tiem Trinh).

i. The Affidavit Fails to Allege a Crime

The 47-page affidavit in support of the search warrant in this case states that, "A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network" and "There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE. …" Ex. 1,

¶ 7. The substance of that access is described as "on May 2, 2019, IP address 24.194.90.108 'was used to access online child sexual abuse and exploitation material' via a website that the FLA named and described as the TARGET WEBSITE." Ex. 1, ¶ 32. As detailed in the affidavit, the "target website" does not contain child exploitation material, but instead contains links to other sites alleged to contain exploitative materials. The IP address having been used to access the target website does not equate to accessing exploitative materials. An alleged visit to the target website, without more, does not allege illegal activity.

Most of the 47 pages are used to explain how the Tor internet server works, and details about how the target website operates. These details do not include any specific allegations that Shacar engaged in any of the conduct described. Paragraph 23 of the affidavit states that "for registered guests, the photo archive is available" making it clear that the photo archive is not available to each and every user who accesses the site, which is what the affidavit alleges Shacar did. Paragraph 32 contains a conclusory allegation that goes further than the earlier reference to Shacar's alleged conduct: the FBI was notified that a Foreign Law Enforcement Agency determined that on May 2, 2019, IP address 24.194.90.108" was used to access online child sexual abuse and exploitation material" via a website that the FLA named and described as the TARGET WEBSITE. How it was determined that Shacar had accessed materials "via" the target website was not discussed in the affidavit, just a bare assertion that he had done so.

Paragraph 16 of the affidavit states that the Target Website was an online chat site. The affidavit fails to show that a link to actual visual depictions of child pornography was accessed by Shacar. Chatting is not criminalized by the statute cited in the affidavit. Without an assertion beyond that Shacar accessed a chat site, there is no basis to believe there is probable cause that evidence of a crime will be found on Shacar's computer.

Paragraph 37 of the affidavit states that, "FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account." However, no claim is made that Shacar registered an account, nor that he accessed a message thread. The affiant does not provide any statistics about how often a person goes to the website after having been given the address (perhaps not even knowing what it is) and is disgusted and flees immediately never to return. But with the facts alleged in the affidavit, such a person could very easily be Shacar. No claim is made as to how much time Shacar spent on the Target Website, nor that he clicked on any of the content of the Target Website. The statistical claim by the affiant, without more facts, does not apply to, nor establish the intent of, this particular user. The affiant seems to acknowledge the lack of facts incriminating Shacar in paragraph 39: "any user who accessed the TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so." The allegation is that Shacar accessed the target website, period. There is no claim that Shacar spent more than a second on the site, that he registered as a user, that he gained access to any files on the site, that he purchased anything on the site, that he downloaded anything from the site, that he followed a link on the site, or that he ever returned to the site – one moment of access, that is all that is alleged against Shacar. This is not sufficient to show probable cause that evidence of a crime will be found on Shacar's computer.

ii. The Affidavit Fails to Establish the Basis of Knowledge for the Tip.

The affidavit is deficient because it failed to establish the basis of knowledge for the tip in two respects. First, Agent Yon did not include any information about whether the tip was obtained through first-hand knowledge or through hearsay. Second, Agent Yon included no facts

about the method used to obtain the IP address information and whether that method was reliable.

The only information provided in the affidavit that offered any clues about the source of the FLA's tip were Agent Yon's statements that the FLA "had obtained [the information in the tip] through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws," and that "FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Ex. 1, ¶ 34. However, neither statement by Agent Yon was sufficient to establish or to assure the Magistrate of the tip's reliability. Agent Yon did not state that the IP address information had reached the FLA through a reliable first-hand source rather than through multiple layers of hearsay. Cf. *Gates*, 462 U.S. at 234 (noting that the informant's "explicit and detailed description of alleged wrongdoing, along with a statement that the event was observed first-hand, entitles his tip to greater weight than might otherwise be the case"); *United States v. Taylor*, 985 F.2d 3, 5-6 (1st Cir. 1993) (noting that an affidavit may support an informant's veracity "through the very specificity and detail with which it relates the informant's first-hand description of the place to be searched or the items to be seized"). Nor did Agent Yon aver that no FLA had "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. 1, ¶ 34. Instead, Agent Yon left the Magistrate to guess at how the FLA had obtained the information and to merely ratify Agent Yon's conclusion that the tip was a reliable one.

The First Circuit has found that a lack of explanation of the basis of knowledge for an informant's tip undermines a finding of probable cause. *Gifford*, 727 F.3d at 99-101. In *Gifford*, an informant told the affiant that the defendant was growing marijuana at his house. Id. at 95. However, the affidavit included no information about the informant's basis of knowledge for the

tip. It was therefore unclear "whether the informant just happened to view the grow operation, heard about it as hearsay, or had direct, first-hand knowledge of the grow operation in the Gifford home." Id. at 100. Because the affidavit lacked any "statements as to the informant basis of knowledge," there was no means for the magistrate to determine "whether that information was obtained first-hand or through rumor." Id. The lack of any information about the source of the informant's knowledge weighed against a reliability finding in *Gifford*.

The facts of this case mirror those in *Gifford* and compel the same conclusion. As in Gifford, it is entirely unclear how, when, and through what method the FLA that provided the tip learned about the IP address. Without that information, there was no basis for the magistrate to determine whether the content of the tip from the FLA was reliable and trustworthy. By not divulging any information about the FLA's basis of knowledge, the magistrate was left with no reason to believe that the tip was obtained through a reliable and trustworthy source or method. Simply repeating the FLA's allegation without further explaining how the FLA uncovered the connection between the IP address and the accessing of child sexual abuse material was insufficient to adequately establish the basis of knowledge of the tip. Thus, the first and second factors of Tiem Trinh – "whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information" and "whether an informant's statements reflect first-hand knowledge" – weigh in Mr. Shacar's favor. *Tiem Trinh*, 665 F.3d at 10.

ii. The Affidavit Reflects No Effort from Law Enforcement to Corroborate the Substance of the Tip.

In addition to the lack of information about the basis of knowledge or reliability of the method used to obtain the IP address, the affidavit does not include any facts that actually or meaningfully corroborated the tip from the FLA that an internet user had "accessed online child sexual abuse and exploitation material via a website." Ex. 1, ¶ 31-32. While Agent Yon did

include a description of the steps U.S. law enforcement took to confirm who lived at [redacted], that investigation only corroborated the fact that someone lived at the physical address associated with the IP address identified by the FLA. None of that investigation corroborated the tip that that particular IP address was used to access child abuse material on May 2, 2019.

In the affidavit, Agent Yon briefly detailed the steps agents took to identify who, if anyone, lived at [redacted]. According to the affidavit, a record check with the Massachusetts Registry of Motor Vehicles (RMV) indicated that Mr. Shacar resided at the subject premises. Additional RMV records indicate that two vehicles were registered to Shacar at the subject premises. Ex. 1 ¶ 43. In addition, those vehicles were observed at the subject premises on different dates. Ex. 1 ¶¶ 44-45. Representatives of Eversource Energy also indicated that service was being provided to Mr. Shacar at the subject premises. Ex. 1 ¶ 46. A check with the United States Postal Service also showed that Mr. Shacar received mail at the subject premises. Ex. 1 ¶ 47.

While this information certainly may have substantiated a claim that Mr. Shacar lived at that address in March 2021, none of it corroborated the allegation made by the FLA – that an internet user at [redacted] had accessed child sexual abuse material in May 2019. See *Gifford*, 727 F.3d at 99-102 (DMV records that confirmed the defendant lived at his address did not corroborate an informant's tip that there was an ongoing grow operation at that address). There was no evidence in the affidavit that the Internet user had any interest in child pornography other than an uncorroborated allegation of a single visit to an unknown part of the target website, which, as argued, is not enough to demonstrate an interest in such material. The affidavit contains no information actually corroborating the unreliable tip from the FLA. The third factor identified in *Tiem Trinh* – "whether some or all of the informant's factual statements

were corroborated wherever reasonable or practicable" – therefore weighs in favor of Mr. Shacar. *Tiem Trinh*, 665 F.3d at 10.

In sum, Agent Yon failed to establish the basis of knowledge for the tip or the reliability of the method used to obtain the information in the tip. Agent Yon also failed to include any facts that corroborated the unreliable tip. The information provided in the affidavit therefore did not create a "substantial basis" for the magistrate to conclude that probable cause existed. *Gates*, 462 U.S. at 238-39.

b. The Warrant Was Stale.

Stale information cannot establish probable cause that evidence of criminal activity will be found at the place searched. *United States v. Grubbs*, 547 U.S. 90, 96 n.2 (2006). Whether information is stale does not depend solely on the number of days between the events described in the affidavit and the issuance of the warrant. *Tiem Trinh*, 665 F.3d at 13–14. Courts look instead at a number of factors, including "the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." Id. (citing *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008)). In cases involving child pornography, courts have often determined that the passage of a significant amount of time between the acquisition of the incriminating information and the obtaining of a warrant does not render the information stale where the magistrate was provided with information supporting a finding that such materials are likely to have been retained by their possessor. See, e.g., *Morales- Aldahondo*, 524 F.3d at 119.

Here, the FBI did not have probable cause to search Mr. Shacar's home in March 2021 when the alleged access to child sexual abuse material occurred in May 2019 – twenty-two months earlier. The affidavit did not include any allegations specific to Mr. Shacar regarding any

propensity or habits of keeping a collection of child pornography. Moreover, the affidavit failed to state what exactly was accessed on the website, whether it was downloaded or saved in any manner, or whether there were multiple visits to the website – facts that might have bolstered probable cause. Cf. *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015) (no probable cause where the affidavit alleged only that "on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography but did not click on any thumbnails to view the full-sized files").

Without more information specific to Mr. Shacar, and without more information about the material allegedly viewed by the suspect user IP address, there was no probable cause to believe that Mr. Shacar's home contained evidence of a crime. Not only was the sole criminal allegation in the warrant twenty-two months old, but any information about the reliability and source of that allegation was absent from the affidavit. The uncorroborated, stale, and unreliable tip was insufficient to establish probable cause. The warrant was unlawfully issued, and all evidence obtained as a result of the search conducted pursuant to the warrant must be suppressed.

II. The Affiant Made Material Omissions and Misstatements and Mr. Shacar is Entitled to a Franks Hearing as a Result.

The Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the

allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *Gifford*, 727 F.3d at 98 (internal quotations omitted). "Suppression of the evidence seized is justified if, at such a hearing, the defendant proves intentional or reckless falsehood by preponderant evidence and the affidavit's creditworthy averments are insufficient to establish probable cause." *United States v. Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015).

The right to a Franks hearing is triggered not only by false statements but also by material omissions. *Id.*; *United States v. Cartagena*, 593 F.3d 104, 112 (1st Cir. 2010). When a defendant alleges a material omission has been made, "[t]he required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. The First Circuit has held that recklessness may be inferred where "the omitted information was critical to the probable cause determination." *Gifford*, 727 F.3d at 98-100.

Special Agent Yon made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth, regarding two key issues. First, Agent Yon made material misstatements about the nature, origin, and reliability of the tip from the FLA. Second, Agent Yon made material omissions about the method(s) used by the FLA to identify the IP address. These misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause. Mr. Shacar is therefore entitled to a Franks hearing.

a. Agent Yon Misrepresented the Nature, Origin, and Reliability of the Tip.

Agent Yon's affidavit relies entirely on his assertion that an FLA notified U.S. law

enforcement that a particular IP address "was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as the Target Website." Ex. 1, ¶ 32-33. There are no other allegations of criminal activity anywhere in the affidavit. However, this fact is inherently misleading and factually incorrect. Agent Yon did not repeat the tip from the [redacted] verbatim. Rather, he added language that misled the magistrate into believing that U.S. law enforcement had more evidence of criminal activity that it did. The exact words of the tip relayed from the [redacted] to U.S. law enforcement regarding the Target Website were:

> On 2019-05-02 05:02:07 (UTC) 24.194.90.108 was used to access online child sexual abuse and exploitation material. This was a chat site which facilitated the sharing of child sexual abuse and exploitation material, stipulating only girls aged 5 - 13. Users were required to enter a username and password but these were only valid for that single login session.

See Ex. 11, p. 2. Agent Yon did not copy or repeat this language into the affidavit. Instead, he stated the following in his affidavit:

> ["FLA"] notified U.S. law enforcement that the FLA had determined that on May 2, 2019, IP address 24.194.90.108 was used to access online child sexual abuse and exploitation material **via a website** that the FLA named and described as the TARGET WEBSITE.

See Ex. 1, ¶32.

While the change may appear slight, its significance in the affidavit was profound. By manipulating the language of the tip, Agent Yon created the impression that the [redacted] and therefore U.S. law enforcement, had information that the IP address was used to visit the Target Website and then used to access child sexual abuse material. The implication in the affidavit is that the internet user associated with that IP address viewed or downloaded the child sexual abuse material available on the Target Website and

possibly that, because the majority of the material was only available through an account, the internet user indeed had such an account and had accessed the child sexual abuse material through that account. However, this wholly misrepresents the substance of the tip from the [redacted]. The [redacted] did not provide any such information, nor did U.S. law enforcement have any such evidence. Rather, the tip from the [redacted] conveyed only that the IP address in question was merely used to access the websites.

Other parts of the affidavit reflect that the [redacted] original tip – that a specific IP address was used to access a website, not material on that website – was and has been, U.S. law enforcement's understanding of the tip See Ex. 1 at ¶ 7 ("There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE; p. 21 ("Evidence Related to Identification of Target that Accessed TARGET WEBSITE); ¶ 40 ("According to publicly available information, IP address 24.194.90.108, which was used to access TARGET WEBSITE on May 2, 2019 was registered to Charter Communications, Inc.").

In altering the language from the tip, Agent Yon also omitted the crucial fact that the homepage of the TARGET WEBSITE did not display any child sexual abuse material. Screenshots of the website provided by the government show that in order to "access" any child sexual abuse material, an individual would have had to navigate past the homepage of the websites See Ex. 11, p. 7, Neither the tip documents nor Agent Yon's affidavit specify what, if any, images, videos, or other materials were viewed, downloaded, or "accessed" in any way. Neither the tip documents nor the affidavit state whether the suspect user IP address did anything beyond accessing the homepages, which contained no contraband images or material. Neither the

tip documents nor the affidavit allege that the individual associated with the IP address had an account on either website, or that that account was used to "access" any materials. In sum, Agent Yon mischaracterized the substance of the tip which was solely that the IP address in question was used to access the target website which did not display any child sexual abuse images or videos on its homepage.

The distinction between the substance of the tip and Agent Yon's rewording of that tip in the affidavit is important. There is a fundamental difference between: 1) evidence of a one- time visit to a website where no images, videos, or links to child pornography materials were either visible or available on the website's homepage, and no such items were viewed and/or downloaded and 2) evidence of an individual accessing that website and then viewing, downloading, or otherwise possessing materials that would have only been accessible once a user navigated past the homepage. See *United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website— which did not require registering an account or logging in—and that even if one inferred that the defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"); *Raymonda*, 780 F.3d at 105. The information the [redacted] to U.S. law enforcement fell squarely into the first category, which, like Falso, was insufficient to establish probable cause.

By manipulating the language in the tip, Agent Yon misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did. Agent Yon's

misrepresentation about the nature of the tip was recklessly made and was "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155-56. Had Agent Yon been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used to visit a website where no child pornography was visible or available on the homepage, the magistrate could not have found sufficient probable cause to issue the warrant. Mr. Shacar is therefore entitled to a Franks hearing on these false and misleading statements.

b. Agent Yon Made Material Omissions Regarding the Method Used by the FLA to Identify the IP Address.

Agent Yon's affidavit indicated that the FLA (the [redacted]) had not "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. 1, ¶ 34. This assurance created the impression that no law enforcement agency, anywhere, had "interfered with, accessed, searched, or seized" data from a computer in the United States. However, an expert declaration submitted in a case seemingly identical to Mr. Shacar's and arising out of the same FLA tip and investigation, suggests that the specific IP address could not have been identified without running a NIT or, alternative, an error-prone and unreliable traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22- 32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2 (attached as Ex. 12). In Professor Murdoch's declaration, he explains that "there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a Network Investigative Technique (which interferes with a user computer)." Ex. 12, ¶ 23. A NIT works "by forcing the user's computer to disclose its IP address by connecting directly to a law-enforcement server without using the Tor network." *Id*. at ¶ 27. A NIT "necessarily interferes with a user's computer wherever it is located." *Id*. at ¶ 32.

Traffic analysis, on the other hand, is a technique that attempts to "identify which user is

communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." *Id*. at ¶17. Before 2016, "traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases." However, in 2016, Tor addressed this issue and introduced a new extension to its software that caused traffic analysis to "introduce more errors, both false positives (where a user is incorrectly identified as having visited the Onion Service) and false negatives (where a user is incorrectly identified as not having visited the Onion Service)." *Id*. at ¶ 19. This measure, and others, have made it "even more difficult to use traffic-analysis to de-anonymize Tor users." *Id*. at ¶ 21.

The use of either technique by the [redacted] or another FLA would significantly undermine the veracity of the affidavit and its probable cause showing. If traffic analysis were used to uncover the IP address, the undisclosed fact that that technique is inherently error-prone would significantly undermine the strength and reliability of the tip from the [redacted] *See id*. at ¶ 22-32. No magistrate, had he or she been aware that this fundamentally unreliable technique was used to obtain the IP address, would find there was probable cause, especially where the tip about the IP address was not corroborated by any other facts.

Alternatively, the use of a NIT would reveal a substantial misrepresentation in the affidavit, which relies on Agent Yon's assurance that no computer in the United States had been searched. The deployment of a NIT is an unlawful warrantless search. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), *aff'd*, 923 F.3d 1 (1st Cir. 2019). Had any law enforcement agency deployed a NIT to obtain the IP address without a warrant, the Magistrate could not have considered the results of that search in the

probable cause analysis. *See United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005) ("[W]hen faced with a warrant containing information obtained pursuant to an illegal search, a reviewing court must excise the offending information and evaluate whether what remains is sufficient to establish probable cause.").

Agent Yon's omissions regarding the method used to obtain the IP address were material because if the omitted information – either that a NIT or an error-prone traffic analysis was used – was included in the affidavit, it would be "sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100. Mr. Shacar is therefore entitled to a *Franks* hearing on this issue as well.

CONCLUSION

On its face, the affidavit fails to establish probable cause. Excising the myriad misrepresentations from the affidavit and adding in the information omitted from the affidavit, it is clear that no Magistrate, had she or he been presented with the reformed affidavit, would have found probable cause. For the above reasons, this Court should suppress all evidence and fruits obtained pursuant to the invalid search warrant and grant Mr. Shacar a *Franks* hearing.

Respectfully submitted,

BENJAMIN SHACAR

/s/ William J. O'Neil

WILLIAM J. O'NEIL
Attorney for the Defendant
280 N. Main St., Ste. 6
East Longmeadow, MA 01028
(413) 224-2694
BBO#:548445

CERTIFICATE OF SERVICE

I hereby certify that true copies of this document will be served on the registered parties through the ECF system on this date January 29, 2025.

/s/ William J. O'Neil
William J. O'Neil
280 N. Main Street, Ste. 6
E. Longmeadow, MA 01028
(413) 224-2694
BBO#: 548445